PROCESS FOR ACTIVATING A NEW WORK GROUP

The process for activating a new Enhanced Security Work Group is displayed below in The Work Group Activation Process Swim Lane Diagram. The set of tasks that the Originator must perform are located in the topmost swim lane labeled 'Work Group Originator'. These tasks are discussed in the sections following the figure.

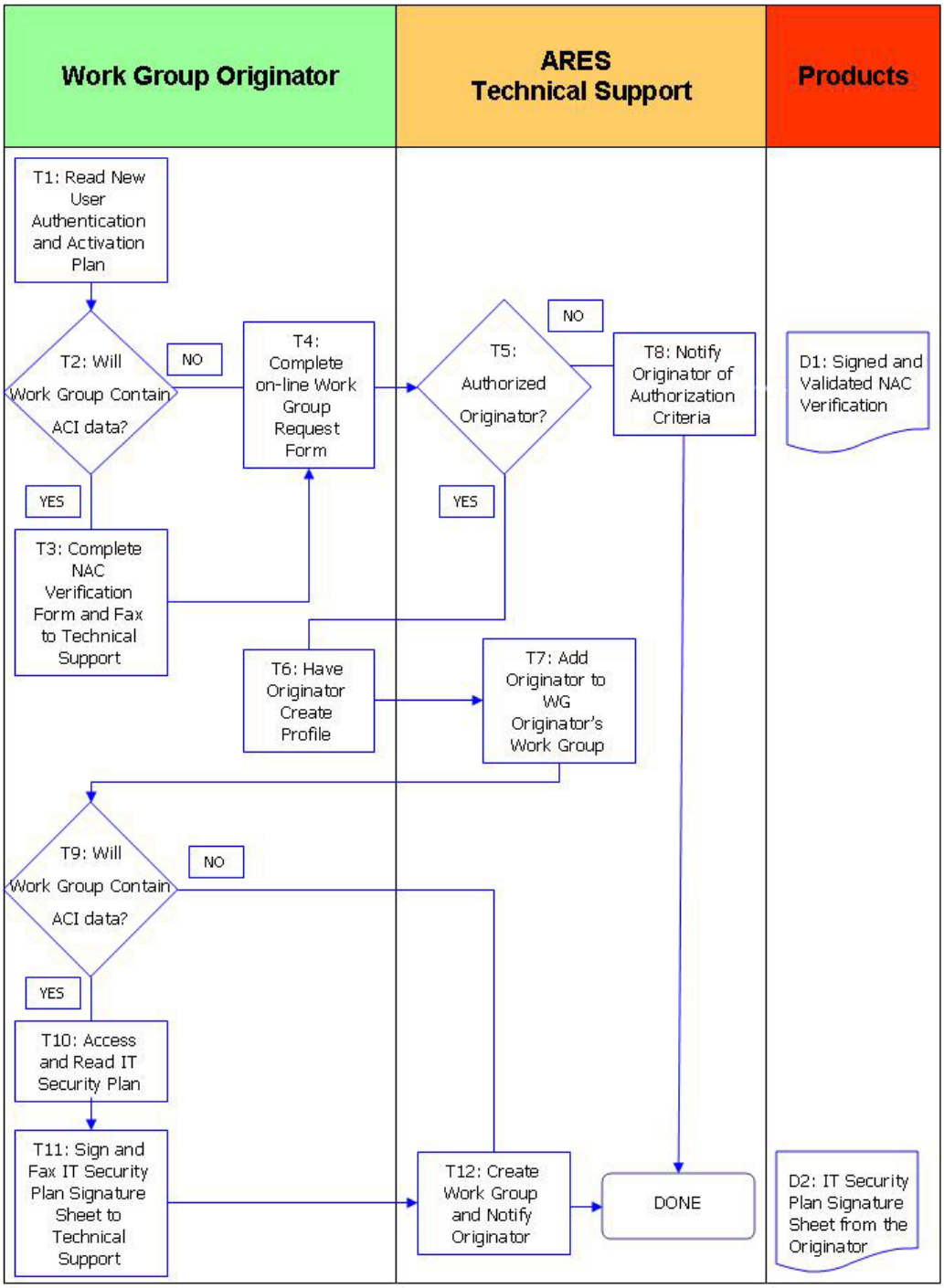

Figure 1: The Work Group Activation Process Swim Lane Diagram

1.1 Read Enhanced Security Work Group NUAAP

STEP T1: The Originator must begin by reading the New User Authentication and Activation Plan (NUAAP), which contains the ESWG General Charter, located in (Appendix A), this document provides the basic procedures to activate a Work Group, and the necessary security practices. The purpose of reading the NUAPP is for the Originator to become familiar with the purpose and responsibilities associated with running a new Work Group.

⇒ The PBMA Program Management reserves the right to deny requests for activation of any Work Group or to delete any existing Work Group that does not comply with the intent of the Enhanced Security Work Groups General Charter.

1.2 Determine Data Content

STEP T2: The Originator must determine if the Work Group will contain Sensitive But Unclassified (SBU) data prior to submitting the request to create the Group. Please note that ACI in the swim lane diagram is synonymous with SBU data. Within NASA and the Federal Government, such information had previously been designated "FOR OFFICIAL USE ONLY." This designation was changed at NASA to "Administratively Controlled Information" (ACI) for clarity and to more accurately describe the status of information to be protected. However, recent efforts to apply consistent terminology across multiple federal agencies have prompted NASA to change the designation to "Sensitive but Unclassified." Please see section 2.4.2 of the NUAAP or NPR 1600.1, *NASA Security Program Procedural Requirements,* Chapter 5.22, which lists the criteria for determining ACI or SBU data. If the Work Group will contain SBU data, continue to complete the NAC Verification Form. If not, continue to section 3.4 of the NUAAP instead.

1.3 Complete the NAC Verification Form

STEP T3: If the Work Group *will* contain SBU data, the Originator must fill out the National Agency Check Verification form located in Appendix B of the NUAAP. The Originator is also responsible for verifying their End-user's ability to access SBU data.

Once completed, the Originator will fax the completed NAC verification form to Technical Support at 440-962-3098.

1.4 Complete Online Work Group Request Form

STEP T4: The Originator can now request a new Enhanced Security Work Group through the PBMA-KMS Web site at http://pbma.nasa.gov/secureworkgroups_main_cid_19. To make this request, perform the following steps:

1. Select a Work Group name.
2. Click the *Request a New Enhanced Security Work Group* tab on the left-hand navigation bar to access the on-line request form.

3. Once you have filled in the required information, click the *Send* button to send the form to Technical Support.

   ⇒ Once a new Work Group request has been granted, the group's Founder or Administrator shall be responsible for the customization of Work Group settings, approval of individuals for membership, and uploading of all default content.

1.5 Create New Profile for Originator

STEP T6: Once the Originator has met the criteria for obtaining a Work Group, Technical Support will send notification to the Originator to create their account. To create this account, perform the following steps:

1. Go to https://secureworkgroups.grc.nasa.gov.
2. Click the "Create an account" link.
3. Fill out the on-line form and click the "Create Account" button to complete the process.

Once the Originator's account is created, it will then be added to the Originator's Work Group. This Work Group has been created for information that pertains specifically to Originators.

1.6 Approvals Required for SBU Capable Work Groups

STEP T9: The Originator must determine if the Work Group will handle SBU data. Each Originator is also responsible for verifying their End-user's ability to access SBU data as per Code I requirements.

Work Groups are available to all NASA and contractor personnel, industry partners and academia. All Originators are required to submit proof of United States citizenship via the National Agency Check Verification form found in Appendix B of the NUAAP.

It is strongly recommended that Originators of Work Groups containing SBU data make *all* End-users complete the National Agency Check Verification form.

1.7 Access the PBMA ESWG IT Security Plan

STEP T10: Once an Originator's request for an SBU-capable Work Group is approved and the Originator has created their account, they will be added to the requested Work Group. They will also be added to the "ACI Originators" user-group. This allows them to access the *PBMA ESWG IT Security Plan* ("IT Security Plan").

⇒ Users of the Enhanced Security Work Groups will only have one account. One user ID and one password will be used for access to all Enhanced Security Work Groups that the user has membership in.

1.8 Sign PBMA ESWG IT Security Plan

STEP T11: Once the Originator accesses and reads the IT Security Plan, they must sign the plan's signature sheet. By signing, the Originator gives consent as the Data Owner for the sensitive information to reside on the Work Group. The signature sheet, with the Originator's original signature, must be faxed to Technical Support at 440-962-3098.

⇒ The Work Group cannot be activated without the Originator's signature on the *PBMA ESWG IT Security Plan*.